

ABSTRACT OF THE DISCLOSURE

Disclosed is a random sequence generating apparatus for generating a sequence of integers. A seed receiving section receives a sequence of integers as a seed. An initialization section provides a transformation section with the received sequence of integers. The transformation section performs predetermined transformation on each of the provided integer sequence to acquire a sequence of integers. A rotation section acquires the number of rotation bits from a part of the acquired sequence of integers, performs a rotation operation on the acquired number of rotation bits with respect to all of or part of the sequence of integers taken as a bit sequence, and acquires a sequence of integers. An updating section provides the transformation section with the sequence of integers. An output section outputs part of a sequence of integers obtained last as a random sequence in case where transformation and rotation are repeated a predetermined number of times.